

Справочные сведения о продукте

Начальное представление о платформе RSA enVision™

Система управления журналами регистрации событий *3-в-1*

Что это такое?

Аналитики, в том числе Gartner, соглашаются с тем, что платформа RSA enVision™ является лидирующей технологией на рынке продуктов управления информационной безопасностью (Security Information and Event Management - SIEM). Эта технология позволяет организации построить единую, интегрированную систему управления журналами регистрации событий по типу «три в одном», упрощая соблюдение отраслевых нормативных требований, повышая безопасность и снижая риски, а также оптимизируя ИТ инфраструктуру и ее обслуживание. Все эти преимущества достигаются благодаря автоматическому сбору, анализу, оповещению об инцидентах, аудиту журналов регистрации событий, подготовке отчетов и надежному хранению всех журнальных файлов.

Назначение

Платформа RSA enVision обеспечивает сбор всех журнальных файлов со всех IP-устройств Вашей сети, при этом постоянно архивирует копии всех полученных данных, обрабатывает журналы в режиме реального времени и генерирует оповещения при обнаружении подозрительного поведения пользователей или устройств. Администраторы через интуитивно понятную инструментальную панель управления могут делать запросы по всему объему сохраненных данных, а развитое аналитическое программное обеспечение преобразует совокупную массу неструктурированных исходных данных в структурированную информацию, формализуя происходящее с целью помочь администраторам в трех главных областях:

Упрощение соблюдения отраслевых нормативов. Администраторы обладают возможностью автоматического сбора данных о событиях в сети, доступе к файлам, приложениям и активности пользователя, что может помочь в подтверждении соответствия отраслевым нормативным требованиям. Для этого заготовлено свыше 1100 встроенных отчетов практически по каждому разделу нормативных требований. Более того, данное решение упрощает достижение соответствия вновь появляющимся требованиям, т.к. сохраняет полный объем данных журналов без какой-либо их фильтрации и нормализации, защищая информацию от намеренного искажения и являясь, таким образом, достоверным источником архивированных данных.

Повышение безопасности и снижение рисков. Оповещение об инцидентах в режиме реального времени, мониторинг и возможность проведения детализированного расследования дают администраторам ясное представление о важных событиях. Благодаря возможности видеть возможные риски и угрозы, а также понимать их значение, они могут предпринимать более эффективные действия по снижению этих рисков.

Оптимизация функционирования IT- и сетевой инфраструктуры. Обработка журнальных файлов - лучший источник информации о производительности различных элементов инфраструктуры и поведении пользователей. Специалисты службы технической поддержки могут использовать платформу RSA enVision для контроля за серверами, сетевыми устройствами и системами хранения, а также для мониторинга сетевых ресурсов, доступности и статуса пользователей, аппаратного обеспечения и бизнес-приложений. Платформа также предоставляет развитый аналитический инструментарий для диагностики сбоев в ИТ-инфраструктуре и защиты сетевых ресурсов, а также значительно упрощает работу ИТ-менеджеров службы «горячей линии», и может до мельчайших деталей показать действия пользователей.

Как это работает?

Платформа RSA enVision позволяет извлекать журнальные файлы одновременно из десятков тысяч устройств, включая Windows®-серверы, межсетевые экраны Checkpoint® и маршрутизаторы Cisco® без установки на них агентов. Это гарантирует, что *все данные* (*All the Data*™) собираются непрерывно и в полном объеме. В то же время набор функциональных возможностей по мониторингу базовых уровней эксплуатации, тенденций, а также генераторы отчетов предоставляют администраторам ретроспективные (в том числе графические) обзоры сетевой производительности и событий безопасности, благодаря чему улучшается эффективность планирования и одновременно снижается трудоемкость данного процесса. Вы можете развернуть платформу RSA enVision либо как автономное «plug-and play» решение, либо как часть масштабируемой отказоустойчивой распределенной архитектуры, характерной для крупномасштабной корпоративной сети. Вне зависимости от выбранного решения, оно будет включать в себя все необходимое программное обеспечение и не потребует каких-либо дополнительных затрат.

Удобный Web-интерфейс управления и технология Event Explorer™ - чрезвычайно развитого аналитического инструмента, обеспечивают интуитивный контроль и возможность углубленного и тщательного расследования инцидентов. Будучи развернутым в качестве автономного решения (серия ES), один функционально полный и защищенный аппаратно-программный комплекс (АПК) обеспечивает выполнение всех функций, включая сбор, обработку, анализ и хранение данных. При развертывании в рамках распределенной архитектуры (серия LS), в требуемых местах устанавливаются специализированные АПК, каждый из которых выполняет свою ключевую задачу: локальные и удаленные сборщики осуществляют сбор данных, серверы данных осуществляют управление собранными данными, а прикладные серверы выполняют анализ данных и генерацию отчетов. Сами данные могут храниться в разработанной компанией EMC непосредственно подключенной системе хранения, находящейся в режиме он-лайн, либо в горячем или холодном резерве.



Какие опции возможны?

Доступные в рамках серий ES и LS варианты моделей базируются на единой аппаратной платформе, но отличаются уровнями лицензий, что позволяет выбрать модель, максимально удовлетворяющую текущим бизнес-требованиям. Для того, чтобы выбрать наиболее подходящий вариант, необходимо оценить количество сетевых устройств, которые Вы должны контролировать, и количество событий в секунду, которое Вам потребуется обрабатывать.

Серия ES		ES 560	ES 1060	ES 2560	ES 5060	ES 7560
Описание		Автономный SIEM АПК	Автономный SIEM АПК	Автономный SIEM АПК	Автономный SIEM АПК	Автономный SIEM АПК
Непрерывный поток (событий/сек.)		500	1 000	2 500	5 000	7 500
Максимальное кол-во контролируемых устройств		100	200	400	750	1 250
Одновременное кол-во пользователей RSA enVision		6	8	10	12	14
Одновременное кол-во пользователей EventExplorer стандартно./макс.		1/5	2/5	3/5	4/5	5/5
Система хранения		300 Гб внутренняя	300 Гб внутренняя	300 Гб внутренняя	Требуется внешняя	Требуется внешняя
Серия LS	**LS A60**	**LS D60**	**LS L605**	**LS L610**	**LS R601**	**LS R602**
Описание	Сервер приложений	Сервер БД	Локальный сборщик	Локальный сборщик	Удаленный сборщик	Удаленный сборщик
Непрерывный поток (событий/сек.)	-	30 000	5 000	10 000	1 000	2 000
Максимальное кол-во контролируемых устройств	-	3 072/6144*	1 500	2 048	512	1024
Одновременное кол-во пользователей RSA enVision	16	-	-	-	-	-
Одновременное кол-во пользователей EventExplorer стандартно/макс.	5/15	-	-	-	-	-
Система хранения	Платформа RSA enVision NAS3500					

Спецификация продукта

ОПЕРАЦИОННАЯ СРЕДА

Защищенный интегрированный Microsoft Windows 2003 Server standard.
Аппаратное дублирование
ES: защищенная ECC RAM.
LS: 8 Гб, полностью буферизованная RAM.
ES/LS: резервные/с горячей заменой вентиляторы, источники питания и диски в конфигурации RAID-1.

МОНИТОРИНГ И УПРАВЛЕНИЕ АППАРАТУРОЙ

Интерфейс внешнего управления IPMI 2.0. Дистанционное управление АПК.

ПОДКЛЮЧЕНИЕ К СЕТИ

ES: 2 порта 10/100/1000TX Ethernet первоначально, возможно расширение до 6
LS: 6 10/100/1000TX Ethernet портов

СТАНДАРТНЫЕ ОПЦИИ СИСТЕМЫ ХРАНЕНИЯ

Непосредственно подключенное устройство полезным объемом 2,75 Тб (см. справочные сведения о RSA enVision DAS2000)
Сетевое устройство полезным объемом 3,5-7 Тб (см. справочные сведения о RSA enVision NAS3500)

ПОДТВЕРЖДЕННЫЕ СООТВЕТСТВИЯ НОРМАТИВАМ

ISO9002, UL1950, CSA22.2 no 950, EN 60950, FCCPart15-Class A, ICES-003
EN55024:1998, EIN55022:1998, EN50082-1, VCCI V-3/2000.4, AS/NZS3548.

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Платформа RSA enVision с LogSmart IPDB; встроенный механизм корреляции событий с автоматическим маркированием угроз; UDS – средство описания еще неизвестных платформе форматов журнальных файлов; более 1100 стандартных отчетов и инструментарий для их создания; инструмент для визуализации данных и анализа инцидентов Event Explorer; средства управления жизненным циклом информации (ILM) платформы RSA enVision включая защиту, управление политикой хранения и поддержку иерархической схемы хранения данных.

ИСТОЧНИК ПИТАНИЯ

С резервированием и распределением нагрузки, 400Вт, автоподстройка 120/240В.

РАЗМЕРЫ И МАССА

29,3 x 17,5 x 3,4 дюйма / 74,4 x 44,5 x 8,6 см (Г x Ш x В).
монтажные салазки в стойку прилагаются (необходима стойка с 4 гнездами).
Масса: 59 фунтов (24,5 кг).

ГАРАНТИЯ

90 дней на аппаратуру с продлением до 5 лет при наличии действующего контракта технической поддержки.



The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

3IN1 DS 0208